

Affidavit in Support of an Application for a Search Warrant

I, Wade M. Brown, being duly sworn, do hereby depose and say:

I am a Criminal Investigator with the Concord, New Hampshire Police Department, where I have been employed since November 2008. Prior to employment with the Concord Police Department, I was employed as a Police Officer with the New York City Police Department from March 2000 through October 2008. I was assigned as a precinct Detective from April 2006 through October 2008, where I received training in interview and interrogation techniques, evidence collection, fraud and identity theft investigations, and homicide and sexual assault investigations. Since July 2018, I have attended over 800 hours of training in digital forensics, to include a six-week Basic Computer Evidence Recovery Training course sponsored by the Department of Homeland Security, and a four-week Mobile Device Examiner course sponsored by the National Computer Forensics Institute. I have received additional digital forensics training from the Internet Crimes Against Children (ICAC) Task Force, the National White Collar Crime Center (NW3C), and Access Data Digital Investigations. Over the course of my law enforcement career, I have participated in hundreds of felony-level investigations and arrests, to include burglaries, robberies, sexual assaults, shootings, and homicides. I also hold a Bachelor's Degree in Administration of Justice from Rutgers University, and I am certified by the New Hampshire Police Standards and Training Council as a full-time law enforcement officer. In April 2016 and again in March 2021, I was sworn in as a Special Deputy Sheriff with the Merrimack County Sheriff's Office. On October 27, 2021, I was sworn in as a Special Federal Deputy Marshal with the United States Secret Service, and may therefore present applications for federal search warrants pursuant to Federal Rule of Criminal Procedure 41.

That as set forth below, the factual basis of the issuance of this warrant is based upon information obtained from this affiant's personal knowledge, observations, and beliefs, information provided to this affiant by other law enforcement officers, my training and experience, and the training and experience of other law enforcement officers assisting in this investigation. This statement does not contain every fact known to me or other investigators. Rather, it contains material information relevant to determining whether there is sufficient probable cause to believe that the specific crimes identified below have been committed.

As the result of an investigation conducted by the Concord Police Department, I have developed probable cause that the violations of 18 U.S.C. § 2251(a) (production of child sexual abuse images); 18 U.S.C. § 2252(a)(1) (transportation of child sexual abuse images); 18 U.S.C. § 2252(a)(2) (receipt and distribution of child sexual abuse images); 18 U.S.C. § 2252(a)(4)(B) (possession of child sexual abuse images) and 18 U.S.C. § 2422(b) (use of a facility of interstate commerce to entice a child to engage in sexual activity), have been committed by Joshua Pincoske. I further attest that there is probable cause to search the information described in Attachment A for evidence relating to these crimes under investigation

I make this statement in support of an application for a search warrant for information associated with certain Snapchat accounts that are stored at premises owned, maintained, controlled, and/or operated by Snap Inc., a communications company incorporated in Delaware and headquartered in Santa Monica, California. The information to be searched is described in the following paragraphs and Attachment A. This statement is made in support of an application for a search warrant under 18 U.S.C. § 2703 to require Snapchat to disclose to the investigating officer records and other information in its possession, pertaining to the subscriber or customer using the service.

As part of this investigation, and pursuant to Title 18 United States Code 2703(f), a preservation request was previously submitted to Snap Inc. through Snapchat's legal team email (lawenforcement@snapchat.com), requesting the preservation of all account contents, IP Logs, any and all Snaps, Stories, Memories, Chats, Location Data, and all other information and data pending the issuance of formal legal process, for the Snapchat Usernames: **hurtkidz** and **strawberry.rum**.

1. **Overview and Initial Involvement by CPD:** In December 2020, investigators from Farmington, NH Police Department began an investigation involving a suspect identified as Joshua Pincoske. Two 17-year-old female juveniles, identified in this statement as Female Juvenile 1 "FJ1" (Born in May of 2003) and Female Juvenile 2 "FJ2" (Born in July 2003), reported inappropriate sexual contact with Pincoske, beginning with online activity and advancing to an in-person incident within the Town of Farmington. It was alleged that Joshua Pincoske paid FJ1 and FJ2 for explicit sexual images transmitted online, as well as for in-person sexual activity inside his vehicle. Pincoske was alleged to have used social media accounts including Facebook, Instagram, Snapchat, Venmo, and Cash App to facilitate the activity.
2. As part of this investigation, on Wednesday, February 2, 2022, a search warrant was executed at the home of Joshua Pincoske at 38 N. Spring Street in Concord, NH. The warrant was executed by Farmington PD, Concord PD, the Merrimack County Sheriff's Office, and members of the NH ICAC Task Force. The search warrant authorized the seizure and forensic examination of Pincoske's digital devices and digital storage media.
3. On that date, Pincoske agreed to a voluntary, non-custodial interview with two detectives, during which he admitted that he knew FJ1 and FJ2, identifying them by their names, and confirming that he solicited sexual images from FJ2 in the past. Pincoske further admitted that he met FJ1 and FJ2 in Farmington and touched their bodies while they sat in his vehicle, but stated that he could not recall if he gave them money. Pincoske denied knowing that FJ1 and FJ2 were under the age of 18 at that time, and stated that he broke off contact when he later found out that they were juveniles.
4. During the execution of the search warrant, multiple digital/electronic devices were recovered which were believed to have been used by Pincoske. These devices were subsequently assigned to the Concord PD Computer Crimes Unit for examination and analysis.
5. **Analysis of Devices and Follow-Up Investigation:** In the days that followed the execution of the search warrant, Detectives Stephen Hemming, Thomas Sheveland, Brendan Ryder and I conducted reviews of the data recovered from three of Pincoske's cell phones as well as his HP Laptop computer. In doing so, several relevant observations were made.
6. Within the data recovered from the HP Laptop (Property #22-497-PR), I observed dozens of apparent screenshots showing a male recognized as Joshua Pincoske engaged in video chats with unidentified naked females using the Omegle website. Omegle is a free online chat service that randomly connects users for one-on-one video chat sessions, and it is known to be used extensively for online sexual encounters.
7. Also, on the HP Laptop, I observed eleven images of a white female juvenile identified here as Female Juvenile 3 "FJ3" (Born in April of 2003). FJ3 was positively identified by detectives based on her involvement and agent familiarity with a specific youth athletic program. The metadata for all eleven images indicate they were from the time frame of April to May 2017, at which time FJ3 was 14 years old. Though some of these images were benign in nature, several others were not and established probable cause to support charges of Sexual Assault (contact) and the

Manufacturing of Child Sex Abuse Material (CSAM) against Pincoske referenced below in paragraph 10.

8. Det. Ryder later found additional Snapchat communications between FJ3 and Pincoske that spanned several years, from December 2017 through November 2019. Though these communications did not include any overtly inappropriate text, they did indicate that attachments and/or images were involved. These attachments were not readily viewable. Det. Ryder discovered that Pincoske's "nickname" for FJ3's Snapchat contact was, "aprettybrowneye." Based on training and experience in Internet Crimes Against Children cases, I am aware that the term "brown eye" is often used to refer to a person's anus.
9. Within a Samsung S8 smartphone (Property #21-510-PR B), multiple images/videos were recovered showing a white female juvenile identified here as Female Juvenile 4 "FJ4" (Born in March of 2004). FJ4 was positively identified based on information contained in the S8, to include her full name and her telephone number. FJ4's identity was further confirmed by law enforcement officers who were personally familiar with her, as well as by two Juvenile Probation and Parole Officers who had worked with FJ4 in the past.
10. I observed photos and/or videos documenting at least 16 separate sexual acts involving Joshua Pincoske and FJ4 from January 2019 through November 2019 (while FJ4 was 14 and 15 years old). Based on the totality of the images, it was believed that they depicted Joshua Pincoske engaging in sexually explicit conduct with FJ4 while she was less than 16 years old. As such, the images/videos were considered evidence of Aggravated Felonious Sexual Assaults (Pattern Offenses) as well as Manufacturing Child Sexual Abuse Images. Based on the evidence recovered involving FJ3 and FJ4, an arrest warrant was obtained and Joshua Pincoske was arrested on February 8, 2022. He has remained incarcerated since that date.
11. Following Pincoske's arrest, the examination of the previously mentioned devices continued to include Pincoske's Samsung S21U smartphone (Property #22-494-PR) and an older Samsung Galaxy 5S smartphone (Property # 22-510-PR-A) The data seen within these devices showed that Pincoske engaged in online conversations with dozens of apparent female teenagers over the past several years. It was also clear that Pincoske utilized applications such as Snapchat, Instagram, Facebook, KIK, and traditional text messages to engage in these communications.
12. KIK is a free mobile messaging application where users can communicate with strangers and enter various chats. It is also an application that is known to promote privacy and anonymity. Through examining the electronic devices seized from Pincoske, Det. Ryder and I discovered that Pincoske engaged in sexual conversations and chatrooms on the KIK application. In many of these conversations, Pincoske openly identified himself and provided personal details consistent with his known information to include name, address, familial status, and his personal interests.
13. During the course of the investigation, Det. Ryder identified several additional *potential* female victims which he designated as FJ5, FJ6, FJ7, and FJ8. Details of those particular female juveniles are not included in this statement, nor should it be inferred that criminal charges are pending in relation to those females. Their existence is documented here merely to explain the jump in numerical designations in the next paragraph.
14. **Discovery of Victim "FJ9":** Within the data recovered from Pincoske's Samsung S21, an unidentified young female was seen who appeared to use the name "Ivy" on KIK and the name "hurtkidz" on Snapchat. Images and videos were observed that depicted "Ivy" engaged in various

sexual acts with many amounting to CSAM. There were also images and videos of an in-person sexual encounter between Pincoske and “Ivy” that appeared to take place on November 12, 2021 at an unknown location. Included in these images was one “selfie” in which Pincoske and “Ivy” can be seen sitting in a vehicle consistent with Pincoske’s vehicle.

15. In light of the Snapchat activity cited above, Det. Ryder sought a New Hampshire state search warrant for Pincoske’s Snapchat account. On July 20, 2022, a search warrant was granted and results were soon obtained from Snapchat in early August 2022. Det. Ryder reviewed this material and later showed me his findings.
16. We observed 279 messages exchanged between Pincoske and “hurtkidz” (a.k.a “Ivy”) between September 13, 2021, and December 7, 2021. Along with the messages, there were 108 attachments which generally consistent of image files. In reviewing the messages, it was clear that a relationship existed between “Ivy” and Pincoske that involved sexualized conversations as well as other on-line meetings on the Omegle platform.
17. With regard to the in-person meeting on November 12, 2021, there were messages from the time period immediately before and after the sexual encounter. The messages documented that Pincoske likely began his journey at or near his home in New Hampshire, was driving to Ivy’s location (believed to be in Massachusetts), and was updating her as he got closer. The messages then stopped for a period of over an hour, consistent with the in-person meeting.
18. The messages then resumed, indicating that they were no longer together. In those messages, “Ivy” indicated that she knew Pincoske had taken pictures and videos and that she wanted to share them with a group. Pincoske responded to her request, saying, “Can I send them to you later once I make sure that there’s nothing incriminating in them LOL.” Based on these messages, it appeared that Pincoske and “Ivy” intended to share CSAM images and videos with others in the KIK Messenger platform. The messages and other phone contents (including photographs) indicate Pincoske likely traveled to his home in New Hampshire later on the evening of November 12, 2021.
19. The final message came from “Ivy” to Pincoske on December 7, 2021, and stated: “its also you that’s gonna be blocked”. I believe this indicated that there was some sort of falling out between “Ivy” and Pincoske, and no further messages were discovered after this point.
20. Within the Snapchat data Det. Ryder also discovered an attachment that Pincoske received from “Ivy” on November 18, 2021. This attachment was an image of a report card from a specific high school in Barnstable County, Massachusetts, indicating that “Ivy” was a sophomore born on June of 2005 and that she resided in a town located in Barnstable County. The messages associated with the report card indicated that Pincoske wanted “Ivy” to attend New Hampshire Technical Institute in Concord, NH. Specifically, “Ivy” stated, “whats that college u wanted me to go to,” and Pincoske replied, “NHTI”.
21. After discovering the report card, Det. Ryder contacted the local police in Barnstable County. In doing so, he confirmed that “Ivy” was the young woman seen in the various media and was also the student indicated on the report card. Det. Ryder confirmed her true identity by reviewing an image from the police department and a school-issued identification showing the same female juvenile; the image on both was consistent with the images of FJ9 discussed above. From this point forward, “Ivy” will be referred to as “FJ9 (Born in June of 2005)”.

22. In October 2022, FJ9 was interviewed by law enforcement. During the interview, FJ9 confirmed a sexual encounter with Pincoske occurred in November 2021. FJ9 identified herself in photographs recovered from Pincoske's S21 cellular phone, and stated that the sexual encounter occurred in the general vicinity of her residence in Massachusetts.
23. In light of the activity on Snapchat between Pincoske and FJ9 and its apparent criminality, Det. Ryder believed that evidence existed on FJ9's Snapchat as well. In an effort preserve this evidence, he submitted a preservation request to Snapchat on September 9, 2022 for the **hurtkidz** account. The time frame of records sought is from September 13, 2021, through December 7, 2021, which are the dates of communication established from Pincoske's messages.
24. **Discovery of Victim "FJ10":** In early August 2022, Det. Brendan Ryder received a call from a Vermont woman identified here as "TN". TN was calling on behalf of her daughter, identified here as "FJ10"(Born in April of 2005). TN advised that FJ10 disclosed to her that she had been involved in an online relationship with Pincoske when FJ10 was between the ages 14-16 years old. TN stated that FJ10's disclosure had been a process that began after FJ10 saw news of Pincoske's arrest in February of 2022. TN further advised that FJ10 had not shared much with her and that she herself knew very little about FJ10's involvement.
25. On August 17, 2022, FJ10 came to Concord to be interviewed at the Merrimack County Child Advocacy Center. Det. Ryder was present in a viewing room to monitor the interview and provided me with the following details:
 - a. During the interview, FJ10 identified Joshua Pincoske by name and said she had initially met Pincoske on an online dating site when FJ10 was fourteen. FJ10 divulged that she would use dating sites to find men who would be willing to pay her for sexually explicit images. FJ10 also advised that she would lie about her age so that men would be willing to solicit images.
 - b. FJ10 said that as with other men, she initially told Pincoske that she was of legal age. However, within the first two video exchanges, FJ10 said that Pincoske questioned whether or not she was 18. FJ10 also said that Pincoske told her that it was "okay" if she was lying about her age and that she could tell Pincoske. FJ10 stated that she then divulged to Pincoske that she was a 14-year-old high school freshman. In response to this, Pincoske asked FJ10 for proof that she was in fact young. FJ10 then provided such prove by showing Pincoske an image of her school identification. On inquiry, FJ10 said that Pincoske's reaction to learning that she was 14 was very "nonchalant" that he was "very okay with it."
 - c. As the interview continued, FJ10 advised that conversations with Pincoske quickly transitioned from the dating application to Snapchat. FJ10 also said that this shift in platforms was Pincoske's idea. FJ10 also said that a portion of these exchanges were saved on her Snapchat account and that as of the week of the interview, they still appeared to be there.
 - d. FJ10 said that the Snapchat exchanges discussed what the images would be and how much they would cost. The conversations also included arranging when FJ10 would be available to video chat. FJ10 added that Pincoske would instruct FJ10 to perform various acts to include "sucking a fake dick" and "putting my fingers in my vagina,"

and that she did so as instructed. FJ10 also confirmed that these messages, images/videos, and video chats occurred over Snapchat.

- e. FJ10 said that Pincoske was “incredibly cheap” and that they would often “go back-and-forth” regarding the price for the images. FJ10 confirmed again that these communications occurred on Snapchat and that her payments were received via Venmo.
- f. FJ10 was asked if she and Pincoske ever had any in-person encounters. FJ10 advised that they did not but that it had been discussed. FJ10 indicated that she was not interested in doing so and that Pincoske tried to ease her concerns about meeting up by letting her know that it was okay and that he had met up with other girls in the past. FJ10 also said that Pincoske stated he would be willing to come pick her up if need be and that FJ10 could lie to her mother to get out of the house.

26. When the interview concluded, Det. Ryder met with FJ10 in an adjacent room to determine if she had any remaining messages or records from Snapchat or Venmo. FJ10 indicated that she did and then showed Det. Ryder the respective applications on her phone. FJ10 further explained that she previously blocked Pincoske, but in preparation for this interview she unblocked him – which resulted in several messages being sent to her phone. Det. Ryder took photographs of the messages displayed on FJ10’s phone screen, and he later showed me these images.

27. Within the Snapchat exchange, it was noted that the discussions transpired as FJ10 had described. Det. Ryder also saw the portion where Pincoske asked for proof of FJ10’s age. The discussion was as follows:

Pincoske: “I have and ID? I want proof you are young”.

FJ10: “Let me find one”

Pincoske: “Love you!!”
“And send me snaps while I am away...Okay”
“I am needy”
“Be a good girl for daddy?”

FJ10: “Ok daddy”

Pincoske: “Doesn’t tell me your age”
“Did it??”
“But I don’t care”
“Love that u are young”
“U have noooooo idea”

FJ10: “it’s shows that I’m in 9th grade”

28. In light of the activity on Snapchat between Pincoske and FJ10 and its apparent criminality, Det. Ryder had probable cause to believe that evidence existed on FJ10’s Snapchat which she identified as “**strawberry.rum.**” In an effort preserve this evidence, he submitted a preservation request to Snapchat on September 9, 2022.

29. Det. Ryder also showed me the images of FJ10's Venmo activity as observed on her phone, which again were consistent with her statement. I observed that Venmo showed an account named Joshua Pincoske which made several payments to FJ10. Pincoske included various emojis with his payments, including a television emoji and a camera emoji. Det. Ryder stated that FJ10 explained the television emoji signified payment for a video, while the camera emoji signified payment for an image. Records obtained directly from Venmo are consistent with the images of FJ10's phone.
30. Based on FJ10's statement, it is believed that the time frame of messages relevant to this investigation will be from approximately April 1, 2019 (the month FJ10 turned 14) through August 17, 2022 (the date of FJ10's CAC interview).
31. **Snap Inc:** I am aware from my training and experience that Snapchat (operating under the name Snap Inc.) owns and operates a communications service that transmits text messages, pictures, and videos from a software application installed on a user's mobile device to another application on the mobile device of one or more users. These messages are referred to by the company, and the people who use the application, as "snaps".
32. Snapchat may be installed and used on tablet or mobile phone including those using Apple's iOS and Google's Android operating systems.
33. Snapchat's differentiating feature from other communications applications is that a sender is able to set a variable amount of time the message is viewable by the receiver. This time can be between one and ten seconds. At the expiration of the time, the message is deleted from Snapchat's servers. Similarly, the message disappears from the user's devices.
34. If the receiver of a Snapchat message does not access the application on their device the message remains undelivered. Snapchat stores undelivered messages for thirty days. After thirty days, the messages are deleted from the company's servers.
35. Before a user can begin employing the features of Snapchat, they must create an account consisting of personally identifiable information and/or information that may provide additional investigative avenues for which additional search warrants or other legal processes may be sought. The initial stage of creating an account is the creation of a unique username. This is the name visible to other Snapchat users. A new user also enters a date of birth. An email address is required to register a Snapchat account. A new user also has to provide a mobile phone number. This phone number is verified during the registration process. Snapchat sends an activation code that must be entered before proceeding with the registration step. Snapchat also retains the account creation date.
36. Snapchat retains log files that are roughly analogous to the call detail records maintained by telecommunications companies. Recorded data includes the date, time, sender, and recipient of a snap. Additionally, Snapchat stores the number of messages exchanged, which users are communicated with the most, message status, (including if and when the message was opened), and whether the receiver used the native screen capture function of their device to take a picture of the snap before it disappeared.
37. Snapchat stores device information such as model, operating system, operating system version, mobile device phone number, and mobile network information of devices used in conjunction with the service. Snapchat also collect unique device identifiers such as the Media Access Control

(MAC) address and International Mobile Equipment Identifier (IMEI) or Mobile Equipment Identifier (MEID) of devices used to access Snapchat. In the event the Snapchat user's application crashes, the company also collects a list of other installed applications on the device to detect any potential software conflicts.


38. If a user consents, Snapchat can access their device's electronic phonebook or contacts list and images. It is unclear if the company stores phonebook information for an extended period or if they simply use it to assist with identifying any other Snapchat users among the contacts.
39. A Snapchat user can keep a sort of photo/video diary using a feature called Story. Each snap is a Story that documents the user's experience. Based on the user's privacy settings, the photos and videos added to the Story can be viewed either by everyone on Snapchat or just the user's friends. Stories are visible to other users for up to twenty-four hours.
40. "Our Stories" is a collection of user-submitted snaps from different locations and events. A Snapchat user, with location services of their device turned on, can contribute to a collection of snaps regarding the event or specific geographic location. Users can also view "Our Stories" events if they are not present at the event by subscribing to the story.
41. Snapchat offers a money transfer service called Snapcash. Users can transfer up to \$2,500.00 per week using this service. Snapcash transactions are only permitted using Visa and Mastercard debit cards issued by a United States Financial Institution. Money transfers can only occur if the sender and receiver both have Snapchat installed and have linked an appropriate debit card to their accounts. To facilitate these transactions, Snapchat retains information about the method and source of payment including debit card information such as card number, expiration date, CVV security code, and billing address zip code. Additionally, the company may have the date of birth and social security number of those involved in money transfers.
42. Based on the foregoing, there is probable cause to believe that 18 U.S.C. § 2251(a) (production of child sexual abuse images); 18 U.S.C. § 2252(a)(1) (transportation of child sexual abuse images); 18 U.S.C. § 2252(a)(2) (receipt and distribution of child sexual abuse images); 18 U.S.C. § 2252(a)(4)(B) (possession of child sexual abuse images) and 18 U.S.C. § 2422(b) (use of a facility of interstate commerce to entice a child to engage in sexual activity), have been violated, and that evidence, fruits and instrumentalities of the offense, more fully described in Attachment A of this statement, will be found within records maintained by Snap Inc. I respectfully request that this Court issue a search warrant authorizing the seizure the items described in Attachment A, to be searched as set forth in Attachment B.

/s/ Wade M. Brown
TFO Wade M. Brown, USSS

The affiant appeared before me by telephonic conference on this date pursuant to Fed. R. Crim. P. 41, and affirmed under oath the contents of this affidavit and application.

Date: **Oct 27, 2022**

Time: **3:42 PM, Oct 27, 2022**

Andrea K. Johnstone 
Andrea K. Johnstone
United States Magistrate Judge

ATTACHMENT A

Contents, data, records, and information associated with Snapchat Usernames, for the applicable timeframes listed:

1. **hurtkidz** (records from September 13, 2021 to December 7, 2021)
2. **strawberry.rum** (records from April 1, 2019 to August 17, 2022)

Snap Chat being a company operating under the name Snap Inc., and headquartered at 2772 Donald Douglas Loop North, Santa Monica CA 90405.

ATTACHMENT B

I. Information to be disclosed by Snap, Inc.

To the extent that the information described in Attachment A is within the possession, custody, or control of Snap, Inc., including any messages, records, files, logs, or information that has been deleted but is still available to Snap, or has been preserved pursuant to a request made under 18 U.S.C.

§ 2703(f). Snap, Inc. is required to disclose the following information to the government that is within the applicable requested timeframes for the accounts listed in attachment A:

1. All contact and personal identifying information, including full name, user identification number, birth date, gender, contact e-mail addresses, Snapchat security questions and answers, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers;
2. Snapchat account login and logout IP addresses and associated time stamps;
3. Originating message IP addresses;
4. Account settings;
5. All files including but not limited to chats, image and videos associated to the Snapchat account;
6. All devices(s) used and otherwise associated with the subscriber's account, including ESN, ICCID, IMSI, IMEI, and MAC address numbers and activation dates;
7. All records of communications and messages made or received by the user, including all private messages, chat history, video calling history, and pending "Friend" requests.

All of the above records are requested in electronic format preferably sent by email or portal to **wbrown@concordpolice.com**

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. § 2251(a) (production of child sexual abuse images); 18 U.S.C. § 2252(a)(1) (transportation of child sexual abuse images); 18 U.S.C. § 2252(a)(2) (receipt and distribution of child sexual abuse images); 18 U.S.C. § 2252(a)(4)(B) (possession of child sexual abuse images) and 18 U.S.C. § 2422(b) (use of a facility of interstate commerce to entice a child to engage in sexual activity), including the following:

- a. Images and videos of suspected child sexual abuse;
- b. Records and information relating to images or videos of suspected child sexual abuse;
- c. Records and information relating to communications between individuals about child sexual abuse;
- d. Records and information relating to membership in online groups, clubs, or services that provide or make accessible child sexual abuse materials to members;
- e. Records and information relating to e-mail accounts used to view, access, trade, distribute, or relay or preserve information concerning child pornography;
- f. Records and information relating to the identity of the user of the accounts, including information relating to how and when and from what devices the account was utilized, including communications with IP addresses, logs, registry entries, configuration file, saved usernames and passwords, email addresses, contacts, photographs, and correspondence.
- g. The identity of the person(s) who created or used the account, including records that help reveal the whereabouts of such person(s).
- h. The identity of the person(s) who communicated with the account, including records that help reveal their whereabouts.